

Leveraging Big Data in Healthcare: Navigating HIPAA, Stark and AKS Compliance, and Security Issues

WEDNESDAY, JANUARY 4, 2023

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Ali A. Jessani, Senior Associate, **Wilmer Cutler Pickering Hale and Dorr**, Washington, D.C.

Ann M. Ladd, Shareholder, **Fredrikson & Byron, P.A.**, Minneapolis, MN

Alaap B. Shah, Member, **Epstein Becker & Green P.C.**, Washington, D.C.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1.**

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail sound@straffordpub.com immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

Recording our programs is not permitted. However, today's participants can order a recorded version of this event at a special attendee price. Please call Customer Service at 800-926-7926 ext.1 or visit Strafford's website at www.straffordpub.com.

EPSTEIN
BECKER
GREEN

WILMERHALE® 

Fredrikson
& BYRON, P.A.

Leveraging Big Data in Healthcare: Navigating HIPAA, Stark and AKS Compliance, Security, and Intellectual Property Issues

January 4, 2023

Strafford CLE Presentation

Speakers



Ann Ladd
Shareholder
Fredrikson & Byron, P.A.

aladd@fredlaw.com

612.492.7124



Alaap B. Shah
Member of the Firm
Epstein Becker Green P.C.

ABShah@ebglaw.com

202.861.5320



Ali Jessani
Associate
Wilmer Hale

Ali.Jessani@wilmerhale.com

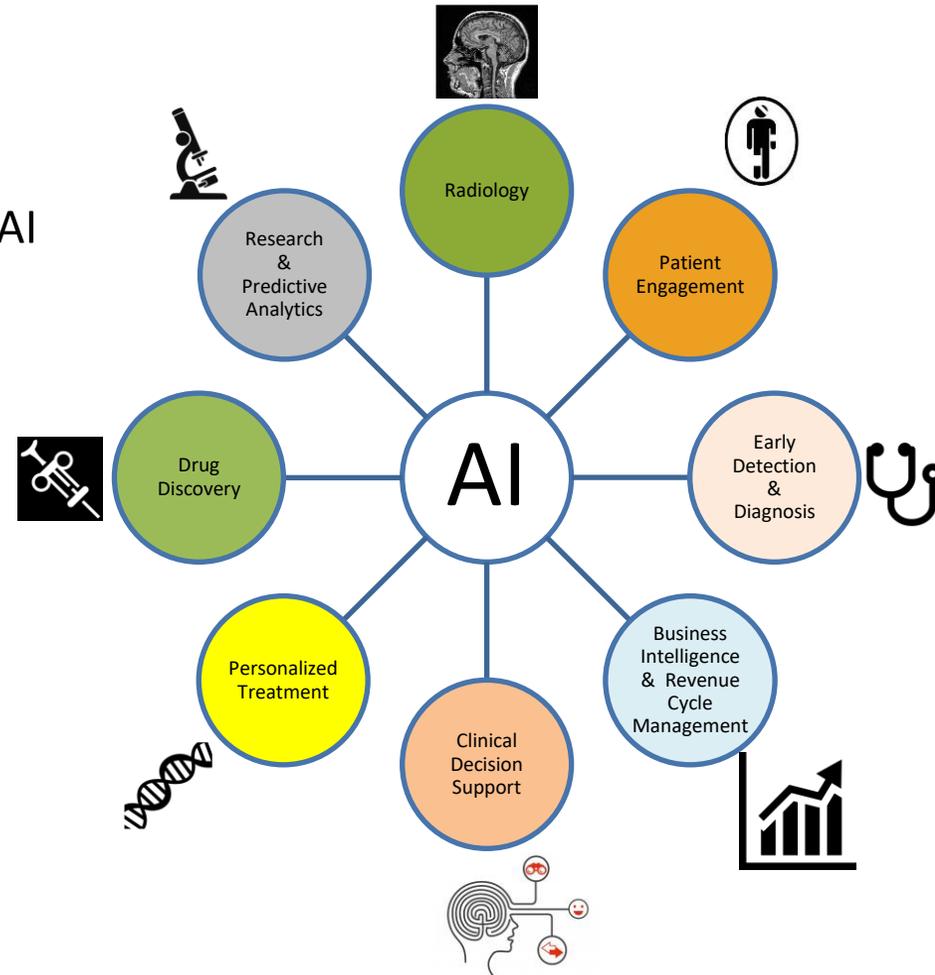
202.663.6105

Agenda

- Introductions
- Setting the Context-
 - Role of AI
 - Examples of “Big Data” in Healthcare
- Legal and Regulatory Issues
 - Privacy and Security
 - Fraud and Abuse
 - Intellectual Property
 - Emerging Ethical Standards for AI/Big Data
- Practical Guidance for Navigating a Big Data Project
- Questions

Case Study #1: Artificial Intelligence

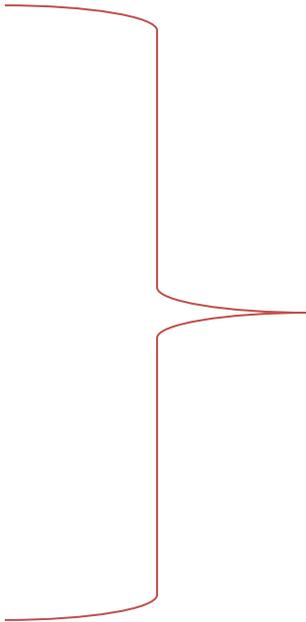
- Rapid digitization coupled with technological advances accelerates development and implementation of AI
- AI value propositions:
 - Generating efficiencies
 - Reducing costs
 - Improving quality and safety
 - Bridging gaps in the continuity care
 - Improving patient engagement
- The United States and China are epicenters of innovation



Case Study #1: Artificial Intelligence (cont'd)

What is AI?

Machine learning
Smart algorithms
Artificial neural networks
Deep learning
Data analytics
Big data
Data mining
Continuously learning system



using computers to analyze data and make decisions by mimicking human “intelligence” but at a greater speed and scale than humanly possible

Case Study #1: Artificial Intelligence (cont'd)

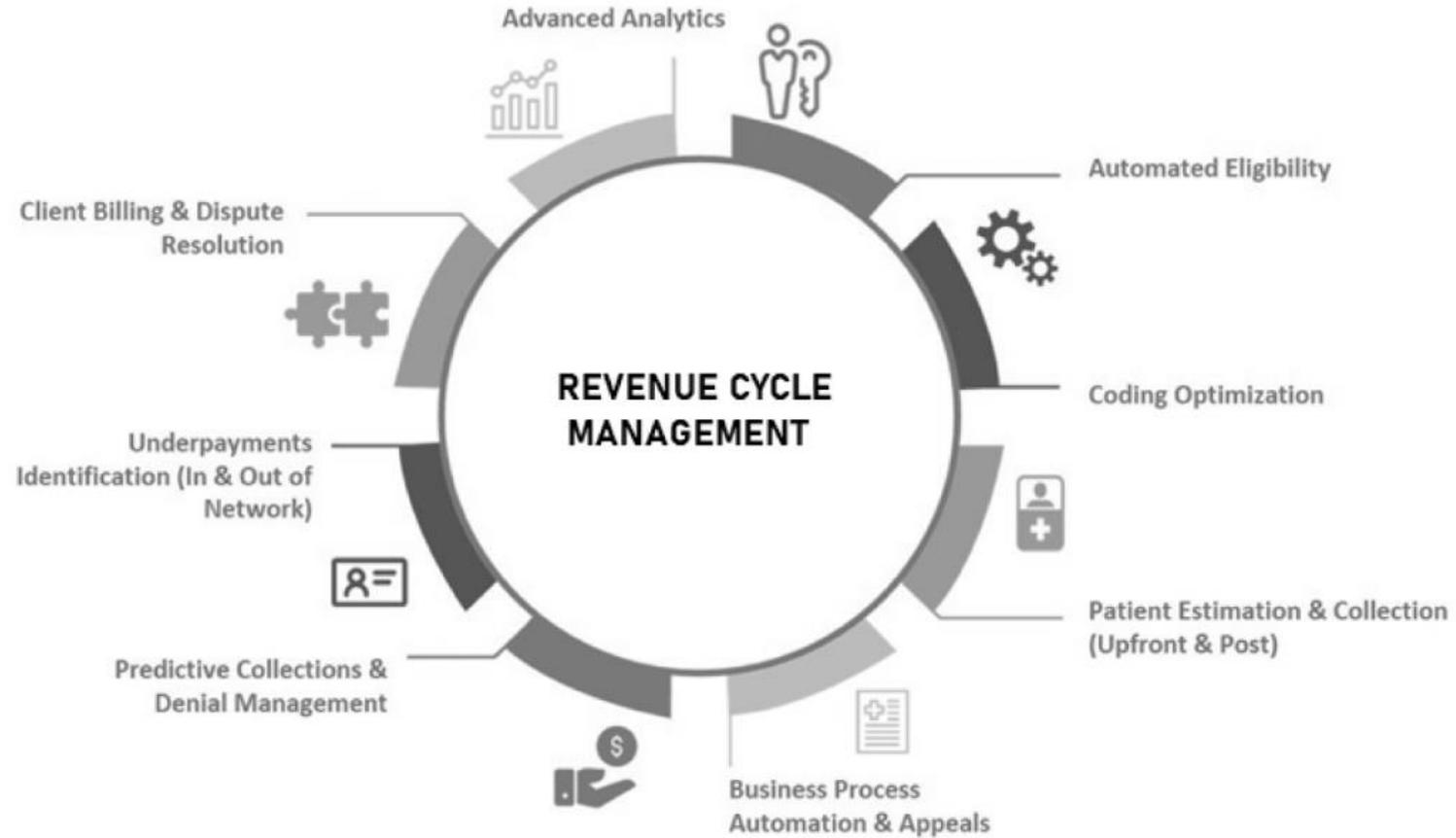
Data is King!

The world's most valuable resource is no longer oil, but data.



- “[Alphabet, Amazon, Apple, Facebook and Microsoft . . . are the five most valuable listed firms in the world.”
- “With data there are extra network effects. By collecting more data, a firm has more scope to improve its products, which attract more users, generating even more data, and so on.”
- “They have a ‘God’s eye view’ of activities in their own markets and beyond.”

Case Study #1: Artificial Intelligence (cont'd)





Case Study #2: Wearable Devices

- Smart watches, health rings, other wearable technology that tracks health information
- Can link data with apps that provide personalized health offerings to consumers based on information collected
- Constantly collect data
- Categories of information collected can include:
 - Fitness tracking
 - Heart rate information
 - Sleep data



Case Study: Wearable Devices (cont.)

- Potential privacy/security issues:
 - HIPAA Compliance
 - Health information regulated as “sensitive” information under comprehensive privacy laws
 - What is health information vs. personal information more generally?
 - More states are regulating health information under their breach notification laws
 - Some data could be considered biometric information
 - IoT data security laws
 - Potential contract issues

Case Study #3-Product Discovery

- AI tools analyzing curated, de-identified data from one or more providers
 - To find/validate new diagnostic tests
 - To support research for new therapies
 - To find new indications for existing products
 - May be structured as a data license or data use agreement

By Susan Barber Lindquist

Mayo, nference expand relationship to increase access to data-derived insights

September 21, 2022



“BIOTIA-DX is our cloud-based metagenomic software which is part of our precision infectious disease detection toolkit. It uses next-generation sequencing and artificial intelligence to reveal a comprehensive microbial (bacteria, viruses, fungi, protozoa) profile, virulence factors, and antibiotic resistance.”

Case Study #3-Product Discovery (cont.)

- Common operational and contractual issues
 - whether to allow use of PHI/PII
 - methods of de- identification
 - evolving standards/restrictions for certain categories of data
 - protecting data sources from unexpected/unwelcome uses of analysis
 - revenue models
 - ownership/rights in IP -new tests/therapies
 - ownership/rights in IP-improvements to AI tools
 - post-termination rights

Health Insurance Portability and Accountability Act (HIPAA)

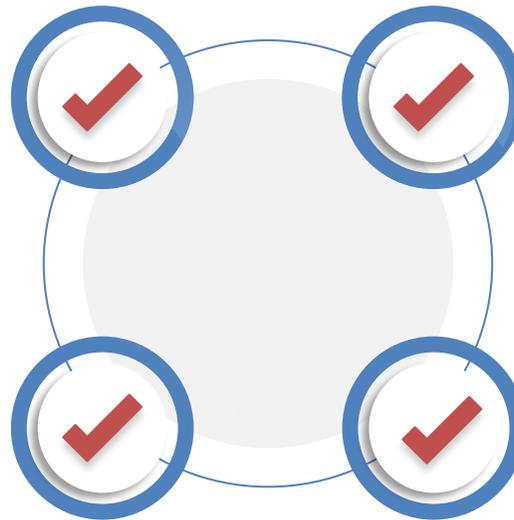


“Your previous provider refused to share your electronic medical records, but not to worry—I was able to obtain all of your information online.”

HIPAA in a Nutshell

The Privacy Rule regulates use or disclosure of Protected Health Information (“PHI”) and obligations to subjects of that information.

The Security Rule sets standards to protect the availability, integrity, and confidentiality of E-PHI



The Breach Notification Rule establishes obligations to report security incidents and breaches to various stakeholders

The Enforcement Rule establishes the penalty framework for HIPAA violations

Who is Subject to HIPAA?

Covered Entities	Business Associates
<ul style="list-style-type: none">• <u>Health care providers</u>: providers of medical or health services who transmit health information in electronic form• <u>Health plans</u>:<ul style="list-style-type: none">○ Health insurers and HMOs○ Insured and self-funded employee welfare benefit plans that have 50 or more participants or are administered by an entity other than the sponsor• <u>Health care clearinghouses</u>: billing services, re-pricing companies and others that engage in data translation	<ul style="list-style-type: none">• Performing functions or provides services involving PHI or maintains PHI on behalf of a Covered Entity• Broad scope of entities considered BAs• Examples:<ul style="list-style-type: none">○ Cloud vendor who hosts PHI○ Data processing involving PHI○ Data analytics involving PHI○ Revenue cycle management○ Patient outreach activities○ Utilization review○ Quality Assurance

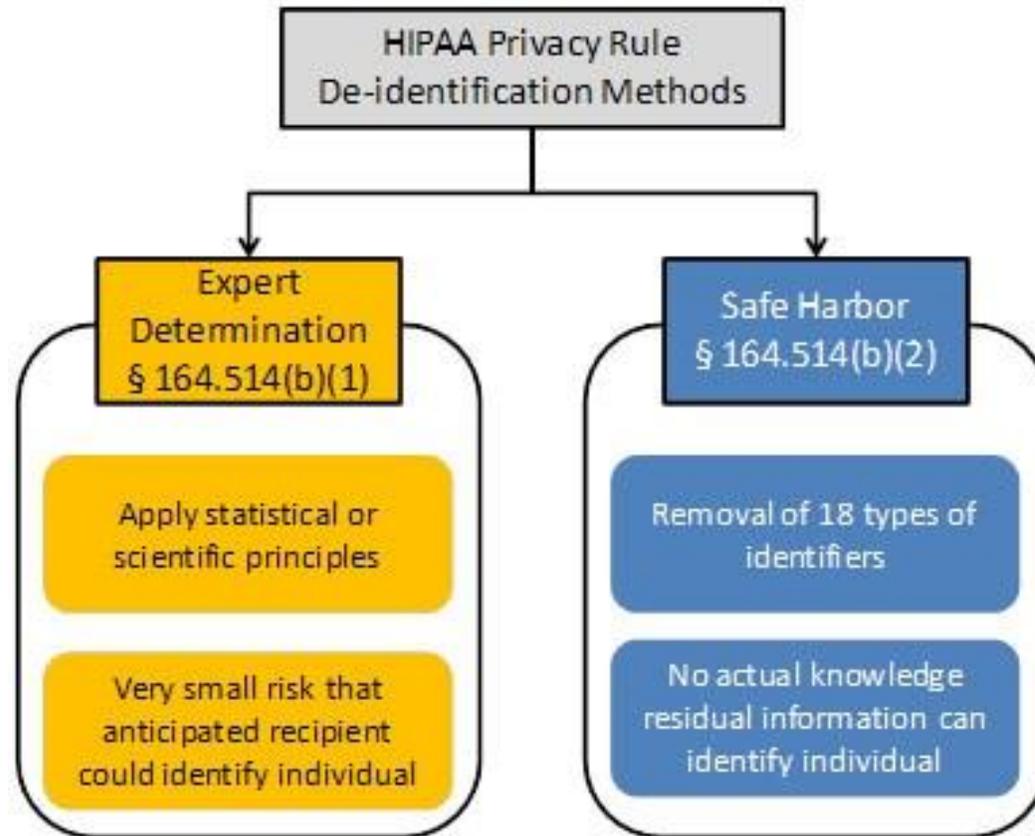
Privacy Rule Basics: Potential Permission to Use and Disclose PHI

General Rule: PHI is confidential, and may only be disclosed with appropriate authorization from the individual

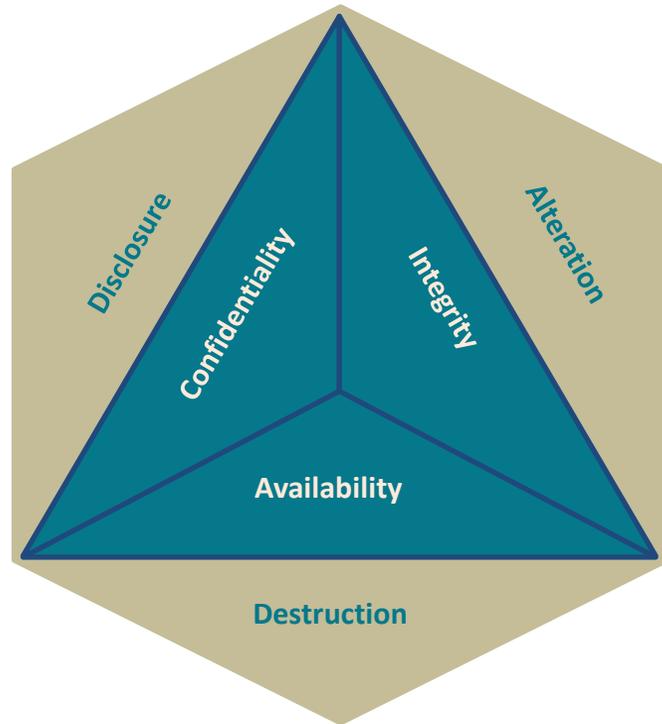
Minimum Necessary: Only the minimum necessary PHI should be used or disclosed to accomplish the intended purpose.

Treatment AI assistance with diagnosis AI assistance with capturing treatment notes	Payment AI assistance with coding AI assistance with making payments
Health care operations AI assistance with analysis of patient population for quality improvement	Research Examining how AI can improve health outcomes

HIPAA De-identification



HIPAA Security Rule Basics



Regulatory compliance and best practices require alignment with the triad of information security

DIRECTLY APPLIES TO BUSINESS ASSOCIATES!

HIPAA Security Rule Safeguard Categories

01

Physical Safeguards

Facility controls, Workstation Security Controls, Device and Media Controls

02

Technical Safeguards

Access Controls, Audit Controls, Integrity Controls, Authentication Controls, Transmission Security

03

Administrative Safeguards

Security Management Processes, Designate a Security Officer, Access/Authorization Processes, Security Awareness and Training, Security Incident Procedures, Contingency Planning

HIPAA Risk Analysis Process

1. Identify the scope of the risk analysis
2. Document threats and vulnerabilities
3. Assess adequacy of current security controls
4. Determine the likelihood of threat occurrence
5. Determine potential impact of threat occurrence
6. Determine the level of risk
7. Identify mitigation strategy
8. Monitor progress of mitigation



False Claims Regulation

False Claims Act (31 U.S.C. §3729)

- A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;
- B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;

Examples of Conduct:

- Direct Submission: knowing submission of false claim
- Indirect Submission: knowingly cause the submission of a false claim
- False certification: knowingly providing false “statements” or “records” to a claim

Knowingly:

- Actual knowledge of the false information
- Acts in deliberate ignorance of the truth or falsity of the information
- Acts in reckless disregard of the truth or falsity of the information

Damages: massive per claim civil penalties, attorney fees, plus treble damages, long look back period

False Claims Risk for RCM Using Big Data/AI



- Providers certify on the CMS 1500 to accurate and complete information
- Inaccurate information can be either errors or false claims, depending on the facts that give rise to the inaccurate information, intent based laws
- Intent can be inferred from facts and circumstances – is the AI used to assist human work or replace it entirely? Degree of reliance is potentially material.
- AI and similar technologies tend to have consistent or clustered errors, rather than random human driven errors
- Enforcement agencies have wide discretion and often treat systemic errors very differently than random:
 - Relevant to intent
 - Assessment of reasonableness of actions (compliance process, corrective actions and standard of care)



Non-HIPAA Privacy Issues for Big Data

- Big Data can be regulated as “personal information” under comprehensive privacy laws
- Open questions include:
 - What information is regulated and what is exempt?
 - What are the standards for deidentification?
 - Are certain use cases regulated? (e.g., targeted advertising)
 - How are data subject access rights executed?



Non-HIPAA Privacy Issues for Big Data

- Five states will have comprehensive privacy laws next year (CA, CO, CT, VA, and UT)
- All of these states regulate health information as sensitive data
- CO, CT, and VA require opt-in consent for processing; CA and UT provide opt-out right
- These laws generally have exemptions for information regulated under HIPAA and Common Rule
- Over 20 states proposed comprehensive privacy laws in 2022 and a similar amount will in 2023



Non-HIPAA Security Issues for Big Data

- Healthcare institutions are increasingly subject to cyber attacks
- Vendors of personal health records are regulated under the FTC's Health Breach Notification Rule
- Definition of personal information under state breach notice laws is expanding to include health information and other categories that could be regulated as Big Data
- State laws require reasonable security for IoT devices
- New state privacy laws requiring reasonable security measures

Intellectual Property Implications of “Big Data” in Healthcare

Not all aspects of data or an algorithm are treated the same

- Underlying data **elements**
- **Compilation** of the data
- Derived or **resulting** data
- **Insights**, other IP generated from access to the data (algorithms trained or improved, other insights/results)
- **Code**
- Machine learning **outputs**

Is Data or AI Protectable by Copyright, Patent or Trade Secret Status? *It depends, and it may not be clear...*

Categories of Intellectual Property

Copyright – (“compilation” – *Feist Publications vs. Rural Telephone Service*)

- An original idea that is put to use (not the idea itself, but the physical use of the idea, e.g., the compilation of data, the written source code. Needs to be more than mere facts...)
- Copyright arises when work written (no need for registration)
- “Works for Hire” concepts
- Author/assignee has the exclusive rights to:
 - Reproduce the copyrighted work
 - Prepare derivative works based upon the work
 - Distribute copies of the work to the public
 - Perform the copyrighted work publicly
 - Display the copyrighted work publicly

Categories of Intellectual Property (cont.)

Patent – covering data (no), vs. database vs. code (maybe—systems and methods of arranging data)...

- What can be patented? Subject matter of the claimed invention must be:
 1. Patent eligible (data structure eligible subject matter?),
 2. Useful,
 3. New;
 4. Non-obvious; and
 5. Described with the particularity required so that people of skill in the relevant technology field or science can understand what the invention is, make the invention and use the invention without “undue experimentation.”
- As issued patent provides a government issued monopoly, e.g., the right to exclude others from:
 - Making (or having made) embodiments of the patented inventions
 - Using embodiments of the patented inventions
 - Selling embodiments of the patented inventions

Categories of Intellectual Property (cont.)

Trade secret protection (state versions of *Uniform State Secrets Act*)

- A trade secret is:
 - Information that has either actual or potential independent economic value by virtue of not being generally known,
 - Has value to others who cannot legitimately obtain the information, and
 - Is subject to reasonable efforts to maintain its secrecy.
- All three elements are required; if any element ceases to exist, then the trade secret will also cease to exist. Otherwise, there is no limit on the amount of time a trade secret is protected.
- The holder of a trade secret has the right to prevent disclosure, acquisition or use of information without consent
- Confidential Know How may be protected by contract even if not a “Trade Secret”

Can “AI” be an Inventor or Author?

Creative works (copyrights) generated by AI? Depends

- USA? No
- Other countries? Maybe



Patent protection for AI-generated inventions?

» No (Dabus)



AI-Generated Portrait Sells for Over \$400K

Intellectual Property Implications of “Big Data” in Healthcare

Bottom line-in the face of uncertainty in the law, make sure your contracts are clear

Be Clear...

- License grants/limitations on use of the data
 - Be specific in the grant of rights- don't rely on IP law concepts.
 - Consider limits related to the term, the scope of the use (purpose), the geography of use, etc.
 - Include clear limitations on use outside the collaboration purposes if that is your intent.
 - Be aware of issues arising from OUS access- IP laws of inventorship/IP concepts may be different.
 - Will you allow sublicenses? If so, how will you manage those?
 - Other authorized users? If so, be clear on responsibility and liability for use.

Be Clear

- Ownership/license rights to 'results'
 - Modified data (structured data, de-identified data)
 - What if the data is combined with data from third parties?
 - Tools used to work with the data
 - Updates to the tools/AI engines
 - Results/insights learned from access

In each case, whether or not you receive ownership rights, consider preserving your own use rights, and understand any limitations on your ability to use, to share with others

Be Clear

- Allocation of IP Risks/Costs Arising from Use
 - Prosecution of patents/protection of trade secrets
 - Understand who is in charge, who bears the cost
 - Defense of Infringement claims – will the provider of AI tools/user of AI tools accessing your data defend you from third party IP claims
 - arising from the use of the AI engines
 - arising from the use of resulting/developed data base
 - arising from the use of developed products

Ethical Use of AI applied to Big Data in Healthcare

- **Concerns:**
 - Data Bias and Algorithmic Fairness
 - Reliability and Safety
 - Informed Consent
 - Accountability, Transparency, and Consent
 - Privacy

Ethical Use of AI applied to Big Data in Healthcare (cont).

- Voluntary and involuntary regulation:
 - FTC Guidance, Blog Posts
 - Industry/Other Guidelines (World Health Organization, Assoc. of British Pharma Industry, AI Councils)
 - Regulations (EU)
 - Internal policies (AstraZeneca, Novartis, Sanofi)

Spotlight on FTC AI Guidance and Enforcement

- Background
 - Section 5 of FTC Act (prohibits unfair or deceptive practices- for instance, use of a racially biased algorithm...)
 - Fair Credit Reporting Act
 - Equal Credit Opp. Act.
- Guidance (April 2020)
 - Be transparent
 - Explain your decisions to the consumer
 - Ensure data and models are robust and empirically sound
 - Hold yourself accountable (compliance, ethics, fairness, nondiscrimination)

Spotlight on FTC AI Guidance and Enforcement (cont)

- Blog Post (April 2021)
 - Start with the right foundation
 - Watch out for discriminatory outcomes
 - Embrace transparency and independence
 - Don't exaggerate claims
 - Tell the truth about uses of data
 - Do more good than harm
 - Hold yourself accountable (“or be ready for the FTC to do it for you”)



Spotlight on FTC AI Guidance and Enforcement (cont)

- Recent Enforcement Actions (Everalbum)
 - Used photos uploaded by app users to train facial recognition. Alleged misrepresentation about ability to delete from app.
 - Consequence– in essence, loss of Intellectual Property:
 - B. Within ninety (90) days after the issuance of this Order, delete or destroy all Face Embeddings derived from Biometric Information Respondent collected from Users who have not, by that date, provided express affirmative consent for the creation of the Face Embeddings, and provide a written statement to the Commission, sworn under penalty of perjury, confirming that all such information has been deleted or destroyed; and
 - C. Within ninety (90) days after the issuance of this Order, delete or destroy any Affected Work Product, and provide a written statement to the Commission, sworn under penalty of perjury, confirming such deletion or destruction.

Practical Guidance for Navigating a Big Data Project in Healthcare

- Include the right resources on your team
 - Privacy officer (consistency with ethical and legal approach to use of PHI, data subject rights, scope of consents)
 - IT (how will 3rd party access data, technical architecture, what role will HCP play in de-identification and/or delivery, where will AI/Software tools reside, what interfaces)
 - IT Security (technical reviews, ongoing assessments)
 - Legal (contracting, legal and regulatory compliance, relationship to other existing contracts, risk allocation and mitigation)
 - Compliance (health law matters, compliance with internal policies)
 - Finance (understanding payment rights, accounting, reporting)
 - De-identification expert?

Practical Guidance for Navigating a Big Data Project in Healthcare

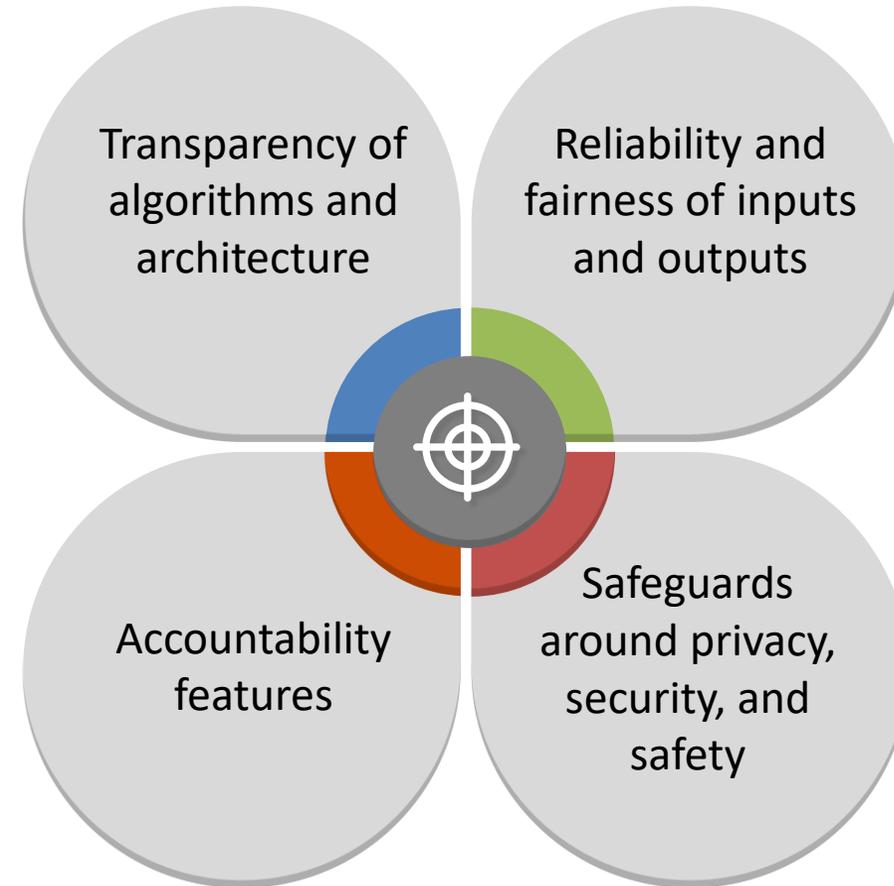
- Decide on your approach to privacy and to data subject rights
 - What standard for removal of identifiers--HIPAA? HIPAA plus GDPR? Impact of other jurisdictions and standards?
 - If you can work only with de-identified (or pseudonymized) data, risks are substantially reduced– under HIPAA:
 - Expert determination
 - Safe harbor (removal of identifiers) by HCP, by BA

Ethical Dimensions for Managing AI Risk

Building TRUST by Opening the AI 'Black Box'



Image credit: Shutterstock



Principles of Good Data Stewardship

- **Transparency**: Provide notice regarding collecting, using, disclosing, and retaining data.
- **Individual Participation**: Engage individuals, and to the extent practicable provide individual with a meaningful choice as to participation.
- **Purpose Specification**: Articulate the purpose(s) for using the data.
- **Data Minimization**: Only collect data that is directly relevant and necessary to accomplish the specified purpose(s) and only retain data for as long as is necessary to fulfill the specified purpose(s).



Principles of Good Data Stewardship (cont'd)

- **Use Limitation**: Use and disclose data solely for the specified purpose(s).
- **Data Quality and Integrity**: To the extent practicable, ensure that data is accurate, relevant, timely, and complete.
- **Security**: Protect data through appropriate security safeguards
- **Accountability and Auditing**: Organizations should be accountable for complying with these principles, providing training to all who use data, and auditing the actual use of data.



Image credit: Shutterstock

EPSTEIN
BECKER
GREEN

WILMERHALE 

Fredrikson
& BYRON, P.A.

Questions?